

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 08-160855

(43)Date of publication of application : 21.06.1996

(51)Int.Cl. G09C 1/00
H04L 9/00
H04L 9/10
H04L 9/12

(21)Application number : 06-298702

(71)Applicant : NIPPON TELEGR & TELEPH CORP
<NTT>

(22)Date of filing : 01.12.1994

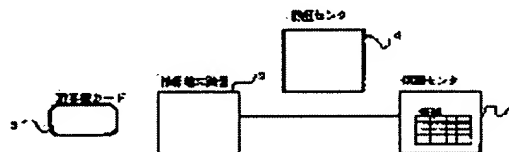
(72)Inventor : TAKASHIMA YOICHI
ISHII SHINJI
YAMANAKA KIYOSHI

(54) DIGITAL INFORMATION PROTECTION SYSTEM AND ITS METHOD

(57)Abstract:

PURPOSE: To provide a digital information protection system and its method without information leaked to a third person and with the difficulty of illegal copying performed by a correct user.

CONSTITUTION: The information identifier of information to be utilized selected from an information terminal device 2 by a user is sent to a calculator card 3 and given a sign, this is transmitted to an information center 1, in the information center 1 a key WK is produced for ciphering the information to be utilized, this is stored in the calculator card 3 via the information terminal device 2, a WK request message including a random number (r) is sent from the information terminal device 2 to the calculator card 3, the stored key WK is set to the information terminal device 2 and the information to be utilized ciphered with the key WK and distributed from the information center 1 is decoded with the set key WK.



LEGAL STATUS

[Date of request for examination] 27.10.1998

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number] 3327435

[Date of registration] 12.07.2002

[Number of appeal against examiner's decision]

of rejection]

[Date of requesting appeal against examiner's
decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平8-160855

(43) 公開日 平成 8 年 (1996) 6 月 21 日

(51) Int. Cl. ⁶	識別記号	庁内整理番号	F I	技術表示箇所
G09C 1/00		7259-5J		
H04L 9/00				
9/10				
9/12				
			H04L 9/00	Z
			審査請求 未請求	請求項の数15 O L (全9頁)

(21) 出願番号 特願平6-298702

(22) 出願日 平成 6 年 (1994) 12 月 1 日

(71) 出願人 000004226

日本電信電話株式会社
東京都新宿区西新宿三丁目19番2号

(72) 発明者 高嶋 洋一

東京都千代田区内幸町1丁目1番6号 日
本電信電話株式会社内

(72) 発明者 石井 晋司

東京都千代田区内幸町1丁目1番6号 日
本電信電話株式会社内

(72) 発明者 山中 喜義

東京都千代田区内幸町1丁目1番6号 日
本電信電話株式会社内

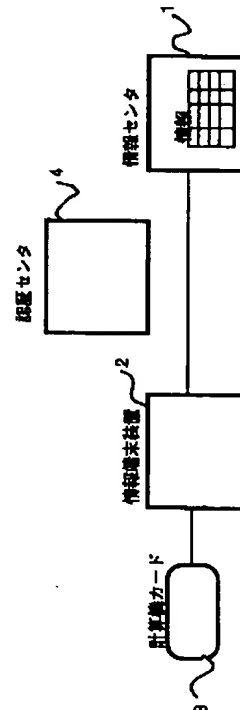
(74) 代理人 弁理士 吉田 精孝

(54) 【発明の名称】 デジタル情報保護システム及びその方法

(57) 【要約】

【目的】 情報が第3者に漏れることなく、正しい利用者であっても違法コピーが困難なデジタル情報保護システム及びその方法を提供する。

【構成】 情報端末装置2から利用者が選んだ利用情報の情報識別子を計算機カード3へ送って署名を受け、これを情報センタ1に送信し、情報センタ1では利用情報を暗号化するための鍵WKを生成し、これを情報端末装置2を介して計算機カード3に蓄積し、情報端末装置2から乱数rを含むWK要求メッセージを計算機カード3に送って前記蓄積された鍵WKを情報端末装置2にセットし、鍵WKで暗号化され情報センタ1から配送された利用情報を該セットされた鍵WKで復号する。



【特許請求の範囲】

【請求項 1】 共通鍵暗号方式もしくは公開鍵暗号方式の公開鍵により暗号化されたデジタル情報を情報センタから通信回線、無線、パッケージメディア等を介して情報端末装置に配送し、事前に情報センタから配布されている計算機カード内の秘密の復号鍵WKで復号しつつ前記デジタル情報を情報端末装置にて利用することを特徴とするデジタル情報保護システム。

【請求項 2】 情報センタは、デジタル情報を蓄積する情報蓄積手段と、情報端末装置との通信を行う通信制御手段と、情報暗号鍵及び復号鍵を生成する鍵生成手段と、デジタル情報を暗号化する暗号化手段と、鍵を暗号通信するための公開鍵暗号化手段と、署名を行うための署名（公開鍵暗号復号）変換手段とを具備したことを特徴とする請求項 1 記載のデジタル情報保護システム。

【請求項 3】 情報端末装置は、情報センタとの通信を行う通信制御手段と、計算機カードとの通信を行う通信制御手段と、デジタル情報を蓄積する情報蓄積手段と、鍵を暗号通信するための公開鍵暗号化手段と、署名を行うための署名（公開鍵暗号復号）変換手段と、乱数を発生する乱数発生手段と、前記乱数と計算機カードから受信した乱数との値を照合する照合手段と、自装置の秘密鍵を格納する秘密鍵蓄積手段と、鍵情報及びデジタル情報を復号する復号手段と、前記乱数発生手段、照合手段、秘密鍵蓄積手段及び復号手段の機密を物理的に保護する機密保護手段とを具備したことを特徴とする請求項 1 記載のデジタル情報保護システム。

【請求項 4】 計算機カードは、情報端末装置との通信を行う通信制御手段と、鍵を暗号通信するための公開鍵暗号化手段と、署名を行うための署名（公開鍵暗号復号）変換手段と、復号鍵WKを格納する復号鍵蓄積手段とを具備したことを特徴とする請求項 1 記載のデジタル情報保護システム。

【請求項 5】 請求項 2 記載の情報センタと、請求項 3 記載の情報端末装置と、請求項 4 記載の計算機カードとを備えたことを特徴とする請求項 1 記載のデジタル情報保護システム。

【請求項 6】 計算機カードと情報端末装置が相互に認証し、計算機カードが利用者を確認し、利用者の要求情報に署名してさらに暗号化して情報センタにアクセスし、利用情報を暗号化するための鍵WKを公開鍵暗号方式で暗号通信して情報利用の前に計算機カードに登録し、鍵WKの受領署名を情報センタへ送信し、情報端末装置から自動的に送付されるWK要求メッセージを受け、その中の乱数を利用して毎回変化する鍵WKの暗号化情報を情報端末装置に送付することにより鍵WKを情報端末装置にセットし、

情報センタからの暗号化情報が情報端末装置に送られると情報端末装置で復号しながら、オンラインでその情報を利用することと、要求情報と鍵WKの受領署名と暗号化情報の受領署名を課金根拠として記録することを特徴とするデジタル情報保護方法。

【請求項 7】 計算機カードと情報端末装置が相互に認証する方法として、情報端末装置が生成した乱数を計算機カードに送り、計算機カードが署名暗号化したものを情報端末装置が受け取り、元の乱数と辻褄が合っているか否かをチェックすることを特徴とする請求項 6 記載のデジタル情報保護方法。

【請求項 8】 計算機カードが情報端末装置を操作する利用者を認証する方法として、予め定めたパスワードを計算機カードに格納しておき、情報端末装置から入力された文字列が一致するか否かをチェックし、入力誤りが所定の回数を越えた時はエラー処理し、該エラーが一定の回数続けて繰り返された場合は計算機カードを無効とするように制御することを特徴とする請求項 6 記載のデジタル情報保護方法。

【請求項 9】 計算機カードが情報端末装置を操作する利用者を認証する方法として、予め定めたパスワードを計算機カードに暗号化して格納しておき、情報端末装置から入力された文字列が暗号化したものと一致するか否か（又は計算機カードに格納された暗号化されたパスワードを復号したものが情報端末装置から入力されたものと一致するか否か）をチェックすることを特徴とする請求項 6 記載のデジタル情報保護方法。

【請求項 10】 計算機カードが情報端末装置を操作する利用者を認証する方法として、予め定めたパスワードを計算機カードに暗号化して又はそのまま格納しておき、情報端末装置から入力された文字列を、情報端末装置と計算機カードとの間で暗号通信し、入力された文字列が暗号化したもの又はそのままのものと一致するか否かをチェックし、一致しているか否かによって生成した乱数のパリティを調節し、その乱数を暗号通信することを特徴とする請求項 6 記載のデジタル情報保護方法。

【請求項 11】 計算機カードが情報端末装置を操作する利用者を認証する方法として、予め定めたパスワードを計算機カードに暗号化して又はそのまま格納しておき、情報端末装置から入力された文字列に情報端末装置で生成した乱数を加えて（あるいは排他的論理和をとって）、情報端末装置と計算機カードとの間で暗号通信し、計算機カードで送られてきた文字列から予め登録してあるパスワードを引き（あるいは排他的論理和をとって）、得られた値を情報端末装置に返送し、情報端末装置で生成した乱数と返送された値とが一致するか否かでチェックすることを特徴とする請求項 6 記載のデジタル情報保護方法。

【請求項 12】 利用者が選んだ情報の情報識別子と情報センタの公開鍵とその証明書とを計算機カードへ送信

し、計算機カードが情報識別子に署名暗号化し、情報端末装置でそれに計算機カードの公開鍵とその証明書を付け加えて情報センタに送信することにより、情報センタへの不正アクセスを防止することを特徴とする請求項 6 記載のデジタル情報保護方法。

【請求項 1 3】 利用情報を暗号化するための鍵 WK を情報センタが生成し、計算機カードの公開鍵で暗号化し、それに対して情報センタの署名を付けて情報端末装置を介して計算機カードへ送り、計算機カードでその署名が正しいか否かを検証し、鍵 WK を得て、該鍵 WK の受領署名を情報端末装置を介して情報センタに送信し、鍵 WK を不正に読み出されないようにして情報識別子とともに蓄積することを特徴とする請求項 6 記載のデジタル情報保護方法。

【請求項 1 4】 情報端末装置が鍵 WK の受領署名を情報センタへ送り出した後、計算機カード内へ乱数 r を含んだ WK 要求メッセージを送信することを特徴とする請求項 6 記載のデジタル情報保護方法。

【請求項 1 5】 計算機カードで WK 要求メッセージ内の乱数と WK を結合し、情報端末装置の公開鍵で暗号化して情報端末装置に送信し、情報端末装置でそれを復号した後、乱数が一致するか否かをチェックし、鍵 WK をセットし、情報センタから送られてくる暗号化情報を復号することを特徴とする請求項 6 記載のデジタル情報保護方法。

【発明の詳細な説明】

【 0 0 0 1 】

【産業上の利用分野】 本発明は、音楽、映像、プログラム等のデジタル情報の不正な複製を防止し得るデジタル情報保護システム及びその方法に関するものである。

【 0 0 0 2 】

【従来の技術】 近年、音声・動画・静止画等のデジタル情報圧縮技術（例えば、MPEG=Moving Picture Experts Group、JPEG=Joint Photographic Coding Experts Group 等）及び ISDN を代表とする高速デジタル通信技術の発達により、音楽・映像・絵画・書籍等の著作物をデジタル情報に変換し圧縮符号化して、情報センタ等から通信回線を介して各利用者端末へ配送することが可能となってきた。

【 0 0 0 3 】 前述した映像等のデジタル情報に比べてデータ量の少ないコンピュータソフトウェアについては、既にパソコン通信等を利用して配送サービスを実施している例がある。また、最近、米国内においてサービスが開始された CD-ROM によるコンピュータソフトの販売方法では、暗号化された販売用ソフト及び暗号化されていないデモ用ソフトを格納した CD-ROM を低価格で販売・配布し、デモ用ソフトを試用した利用者が購入希望を電話等でサービスセンタに申込むと、該利用者に復号鍵を通知して暗号化された販売用ソフトの使用

を可能とする形式をとっている。

【 0 0 0 4 】

【発明が解決しようとする課題】 前述した従来のパソコン通信等によるソフトウェアの販売方法の場合、ソフトウェアの暗号化がなされておらず、フロッピーディスク等のパッケージによるソフトウェアの販売方法に比べて、違法コピーをより容易にさせる環境を提供してしまうという問題があった。

【 0 0 0 5 】 また、前述した CD-ROM によるソフトウェアの販売方法の場合、電話等にて復号鍵をサービスセンタより受け取る際にセンタオペレーションを介するため、人手がかかり、かつ利用者のプライバシーを保つことができないという問題があった。また、人手を介するため、復号鍵の横流し等の不正により違法コピーが可能になるという問題があった。

【 0 0 0 6 】 本発明の目的は、情報が第 3 者に漏れることなく、正しい利用者であっても違法コピーが困難なデジタル情報保護システム及びその方法を提供することにある。

【 0 0 0 7 】

【課題を解決するための手段】 本発明では前記目的を達成するため、物理的に封印された装置を情報端末装置に入れ、復号するための鍵 WK を計算機カードに蓄積し、利用した証拠として、要求情報、鍵受領署名、情報受領署名を情報センタが記録することを特徴とする。

【 0 0 0 8 】

【作用】 本発明によれば、情報を暗号化して配送しているため、情報が第 3 者に漏れる恐れがなく、また、復号鍵が計算機カードの中に閉じ込められており、正しい利用者ですら復号鍵を知ることが困難であり、情報端末装置に物理的に封印してある装置で鍵 WK の復号、情報の復号を行うため、違法コピーが困難であることから、情報提供者が安心して利用できるシステムとなる。

【 0 0 0 9 】

【実施例】 図 1 は本発明のデジタル情報保護システムの一実施例を示すもので、図中、1 は情報センタ、2 は情報端末装置、3 は計算機カード、4 は認証センタである。

【 0 0 1 0 】 情報センタ 1 は、情報提供者から供給された多数のデジタル情報を蓄積し、これをデータベースのように管理している。

【 0 0 1 1 】 情報端末装置 2 は、デジタル情報を利用するための画像表示装置、音声出力装置等を具備し、各利用者の家庭等に配置されている。情報センタ 1 と情報端末装置 2 とは通信ネットワークを通じて相互通信可能のように接続されている。

【 0 0 1 2 】 計算機カード 3 は、情報端末装置 2 に対して着脱自在に取り付けられ、どの情報を購入したかという取引内容を示すデータを内部に蓄積しておくことができる。この計算機カード 3 は利用者毎に所持するこ

とができ、各利用者はこの計算機カード3を情報端末装置2に接続することによって、購入済のデジタル情報（画像、音楽等）を情報センタ1から情報端末装置2に送らせて利用することができる。

【0013】なお、認証センタ4は公開鍵暗号方式を利用する際の準備段階でのみ必要となる。

【0014】（情報センタの構成）図2は情報センタの詳細な構成を示すもので、図中、11は利用情報を入力する情報入力部、12は利用情報を蓄積する情報蓄積部、13は利用情報を暗号化する情報暗号化部、14は利用情報を暗号化する時に用いる鍵WKを生成するWK生成部、15は鍵WKを暗号化する公開変換部、16は暗号化された鍵WKが情報センタのものであることを示すための署名変換部、17は情報センタの公開鍵やその認証センタによる証明書や演算の途中結果等を記憶するためのメモリ、18は情報センタ全体の制御とハッシュアルゴリズムを実行するCPU、19は計算機カードの公開鍵等を検証する公開鍵検証部、20はネットワークとのやりとりを行うネットワーク入出力部である。

【0015】（情報端末装置の構成）図3は情報端末装置の詳細な構成を示すもので、図中、21は計算機カード3とのやりとりを行うカード入出力部、22は公開鍵暗号の復号を行う復号鍵抽出部、23は利用情報の復号を行う情報復号部、24は復号された情報を出力する情報出力部、25aは画像表示装置、25bは音声出力装置、26は復号鍵抽出部22、情報復号部23及び情報出力部24の機密を物理的に保護する機密保護手段、27は利用情報を暗号化されたまま蓄積する情報蓄積部、28はネットワークとのやりとりを行うネットワーク入出力部、29は情報端末装置の公開鍵や認証センタの証明書や演算の途中結果等を記憶するためのメモリ、30は情報端末装置全体の制御と乱数生成やハッシュアルゴリズムを実行するCPUである。

【0016】（計算機カードの構成）図4は計算機カードの詳細な構成を示すもので、図中、31は認証センタの証明書で公開鍵が正当であることを検証する公開鍵検証装置、32は暗号化や署名変換を施す公開鍵暗号装置、33は情報端末装置2との通信を行う通信装置、34は利用者認証のためのパスワード照合を行うパスワード照合装置、35は購入情報の復号鍵を登録する復号鍵登録装置、36は計算機カードの公開鍵やその証明書や演算途中結果を記憶するメモリ、37は計算機カード全体の制御と乱数生成等を行うCPU、38は秘密鍵等の情報を保持するために必要な電圧監視装置、39はバックアップ用の電池である。

【0017】（情報利用プロトコル）

<事前準備>情報Mを鍵Kで暗号化して暗号化情報Cを得る変換を $C = EK(M)$ で表し、復号することを $M = DK(C)$ で表す。特に公開鍵暗号方式を利用する時は暗号化を $C = EK_p(M)$ 、復号を $M = DK_s(C)$ で表

す。後者は署名変換としても用いることがある。

【0018】計算機カード3には予め識別子IDUと公開鍵KPUとその証明書XPUと認証センタ4の公開鍵KPCと秘密鍵KSUとが書き込まれており、特に秘密鍵KSUは読み出せないように保護されたエリアに書き込まれる。証明書XPUは認証センタ4で公開鍵KPUを認証してもらい、 $XPU = DK_s(C(XPU))$ として求められる。但し、KSCは認証センタ4の秘密鍵で、これは認証センタ4以外には秘密にされる。

【0019】同様に、情報端末装置2には予め識別子IDSと公開鍵KPSとその証明書XPSと認証センタ4の公開鍵KPCと秘密鍵KSSとが書き込まれ、情報センタ1には予め識別子IDMと公開鍵KPMとその証明書XPMと認証センタ4の公開鍵KPCと秘密鍵KSMとが書き込まれる。また、計算機カード3には利用者を認証するための情報（例えばパスワード）が読み出されないように登録される。

【0020】<計算機カード・情報端末相互認証>図5は計算機カード・情報端末相互認証の工程を示すものである。

【0021】計算機カード3が情報端末装置2に接続されると、情報端末装置2から、乱数Rと該情報端末装置2の公開鍵KPSとその公開鍵の証明書XPSと該情報端末装置2の識別子IDSとが計算機カード3へ送られる。

【0022】計算機カード3はその内部に保持している認証センタ4の公開鍵KPCを利用して、情報端末装置2の公開鍵KPSとその証明書XPSとの辻褄が合っているか否かを確認することにより、情報端末装置2の公開鍵KPSが正当であるか否かを判断する。正当と判断された時は送られて来た乱数Rに署名暗号化変換を施し、 $T = EK_p(DK_s(R))$ （又は $DK_s(EK_p(R))$ ）なるTと計算機カード3の公開鍵KPUとその証明書XPUと識別子IDUとを情報端末装置2に送信する。

【0023】情報端末装置2はその内部に保持している認証センタ4の公開鍵KPCを利用して計算機カード3の公開鍵KPUが正当であることを確認した後、送られてきたTと送ったRとの辻褄が合っているか否かを確認することにより、相手が正しい計算機カードIDUであるか否かを判断する。

【0024】<利用者認証>図6は利用者認証の工程を示すものである。

【0025】利用者は、情報端末装置2に予め計算機カード3に登録してあるパスワードを入力する。情報端末装置2は入力されたパスワードを計算機カード3に送信し、正しいかどうかを判断してもらう。パスワードの入力が正しい場合には、正当な利用者であると判断し、メニュー情報を利用者に示す。

【0026】この際、パスワードの入力誤りは予め定めた所定の回数、例えば3回まで許容し、3回を越えた時はエラー処理、つまり正当な利用者でない可能性がある

として計算機カード3を排出し、さらに該エラーが予め
 定めた一定の回数、例えば5回続けて繰り返されたよう
 な場合は正当な利用者でないとして該カードを無効とす
 る。

【0027】なお、利用者認証の別の方法として、予め
 定めたパスワードを計算機カードに暗号化して格納して
 おき、情報端末装置から入力された文字列が暗号化した
 ものとは一致するか否か（又は計算機カードに格納され
 た暗号化されたパスワードを復号したものが情報端末装
 置から入力されたものとは一致するか否か）をチェックす
 る方法、予め定めたパスワードを計算機カードに暗号化
 して又はそのまま格納しておき、情報端末装置から入力
 された文字列を、情報端末装置と計算機カードとの間で
 暗号通信し、入力された文字列が暗号化したもの又はそ
 のままのものとは一致するか否かをチェックし、一致して
 いるか否かによって生成した乱数のパリティを調節し、
 その乱数を暗号通信する方法、予め定めたパスワードを
 計算機カードに暗号化して又はそのまま格納しておき、
 情報端末装置から入力された文字列に情報端末装置で生
 成した乱数を加えて（あるいは排他的論理和をとって）、
 情報端末装置と計算機カードとの間で暗号通信し、計算
 機カードで送られてきた文字列から予め登録してあるパ
 スワードを引き（あるいは排他的論理和をとって）、得
 られた値を情報端末装置に返送し、情報端末装置で生
 成した乱数と返送された値とが一致するか否かでチェック
 する方法等が適用できる。

【0028】<利用者選択>図7は利用者選択の工程を
 示すもので、利用者はメニュー情報から必要な情報を
 選ぶ。

【0029】<情報要求>図8は情報を要求する情報要
 求の工程を示すものである。

【0030】利用者は選んだ情報の情報識別子Req（音
 楽情報の場合、国際レコーディングコード（ISRC）
 等の全世界共通コードや、情報提供者が独自に付与し
 た情報を一意に特定できる番号等）と情報センタ1の公
 開鍵KPMとその証明書XPMとを計算機カード3へ送信す
 る。

【0031】計算機カード3は認証センタ4の公開鍵K
 PCで情報センタ1の公開鍵KPMとその証明書XPMとの辻
 褁が合っていることを確認し、Reqに署名暗号化し、 R
 $U = E_{K_{P_U}}(DK_{S_U}(Req))$ なるRUを情報端末装置2に
 送信する。

【0032】情報端末装置2はRUを受けると、それ
 に計算機カード3の公開鍵KPUとその証明書XPUとを付
 け加えて情報センタ1に送信する。

【0033】情報センタ1は送られてきた計算機カード
 3の公開鍵KPUとその証明書XPUとの辻褁が合っている
 ことを確認し、RUからReqを $Req = E_{K_{P_U}}(DK_{S_U}(R$
 $U))$ として求め、情報を検索する。

【0034】<鍵配送・鍵受領署名>図9は鍵配送・鍵

受領署名の工程を示すものである。

【0035】利用情報を暗号化するための鍵WKを情報
 センタ1が生成し、計算機カード3の公開鍵KPUで暗号
 化し、 $CK = E_{K_{P_U}}(WK)$ なるCKに対して署名を施
 し、 $SKM = DK_{S_U}(CK)$ なるSKMとCKとを情報端末
 装置2を経由して計算機カード3へ送信する。

【0036】計算機カード3はその署名が正しいかどう
 かを検証し、CKを復号することにより鍵WKを得て、
 鍵WKの受領署名として $SU = DK_{S_U}(SKM)$ なるSU
 を、情報端末装置2を経由して情報センタ1に送信す
 る。鍵WKは不正に読み出されないようにして、情報識
 別子とともに蓄積する。

【0037】<鍵WK要求>図10は鍵WK要求の工程
 を示すものである。

【0038】情報端末装置2はSUを情報センタ1へ送
 り出した後、計算機カード3へ乱数rを含んだWK要求
 メッセージReqWを送信する。

【0039】<情報配送・情報利用>図11は情報配送
 ・情報利用の工程を示すものである。

【0040】計算機カード3はReqW内の乱数rと鍵W
 Kを結合して情報端末装置2の公開鍵KPSで暗号化し、
 $V = E_{K_{P_S}}(WK, r)$ なるVを情報端末装置2に送信
 する。情報端末装置2ではVをKSSを用いて復号した
 後、rが一致するか否かをチェックし、鍵WKをセット
 する。

【0041】一方、情報センタ1は鍵受領署名SUを受け
 とると、情報Iを処理単位に分割し、その単位毎に前記
 鍵WKで暗号化し、 $C = E_{WK}(I)$ なるCにハッシュ関
 数h()を施し、署名し、 $SIM = DK_{S_U}(h(C))$ なる
 SIMとCとを情報端末装置2へ送る。情報端末装置
 2ではその署名が正しいことを検証し、暗号化情報Cを
 復号する。

【0042】なお、KSSを用いて復号する装置からWK
 で復号する装置までは物理的に機密保持がなされてい
 る。その実現方法としては該部分を頑丈な容器に入
 れ、封印をするか、R.Mori and M.Kawahara 'Superdist
 ribution: The Concept and theArchitecture' Trans.
 IEICE, E-73, No. 7, 1990-7に記載された方法を適用す
 ることが可能である。

【0043】Cが復号できたら、それに情報端末装置2
 の署名をして情報センタ1に $ACK = DK_{S_U}(h$
 $(C))$ を返す。情報センタ1はACKが正当なもので
 あることを確認した後、RU, SU, ACKを課金根拠と
 して記録する。ACKが帰ってくることを確認して、次
 の処理単位について処理を継続する。

【0044】なお、前記実施例ではISDN等の公衆通
 信回線を利用する場合について示したが、専用線等のコ
 ネクションレスの回線にも適用できることはいうまでも
 ない。

【0045】

【発明の効果】以上説明したように本発明によれば、暗号化された情報本体と復号鍵を分離し、かつ、復号鍵を計算機カード内に安全に格納することにより、情報が第三者に漏れることがないことと、違法コピーが困難であることから、情報提供者が安心して利用できるシステムを構成でき、しかも利用者にとって不利になることはなく、利用したい情報が近くの情報端末装置に無くとも、情報センタへアクセスすることにより利用でき、また、どの情報端末装置からでも利用可能となる等の利点がある。

【0046】なお、本発明は、コンピュータソフトウェアのみならず、全ての暗号化デジタル情報の通信利用による配送の際に適用できることは言うまでもない。

【図面の簡単な説明】

【図1】本発明のデジタル情報保護システムの一実施例を示す図

【図2】情報センタの詳細な構成図

【図3】情報端末装置の詳細な構成図

【図4】計算機カードの詳細な構成図

【図5】計算機カード・情報端末相互認証の工程を示す図

【図6】利用者認証の工程を示す図

【図7】利用者選択の工程を示す図

【図8】情報を要求する情報要求の工程を示す図

【図9】鍵配送・鍵受領署名の工程を示す図

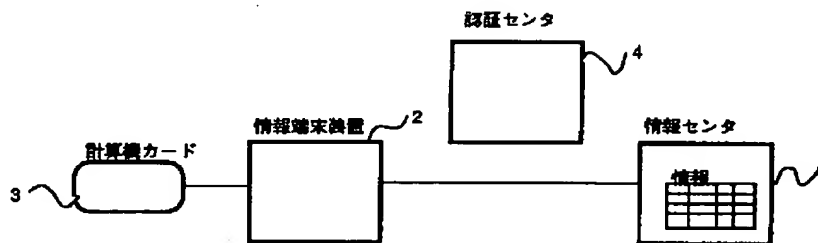
【図10】鍵WK要求の工程を示す図

【図11】情報配送・情報利用の工程を示す図

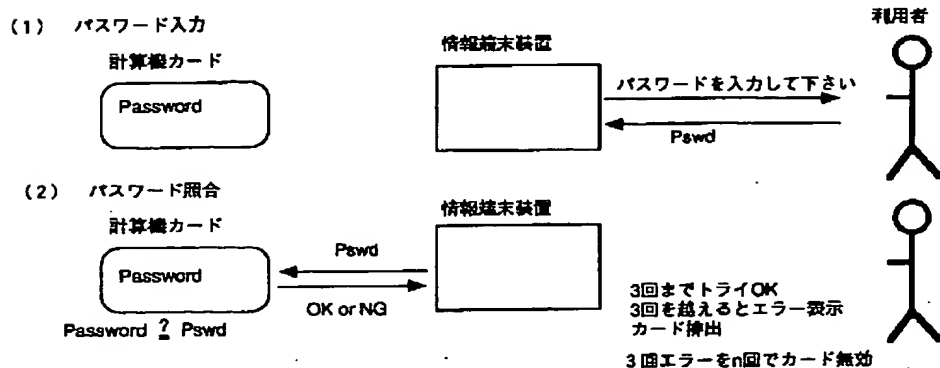
【符号の説明】

1…情報センタ、2…情報端末装置、3…計算機カード、11…情報入力部、12…情報蓄積部、13…情報暗号化部、14…WK生成部、15…公開変換部、16…署名変換部、17…メモリ、18…CPU、19…公開鍵検証部、20…ネットワーク入出力部、21…カード入出力部、22…復号鍵抽出部、23…情報復号部、24…情報出力部、25a…画像表示装置、25b…音声出力装置、26…機密保護手段、27…情報蓄積部、28…ネットワーク入出力部、29…メモリ、30…CPU、31…公開鍵検証装置、32…公開鍵暗号装置、33…通信装置、34…パスワード照合装置、35…復号鍵登録装置、36…メモリ、37…CPU、38…電圧監視装置、39…電池。

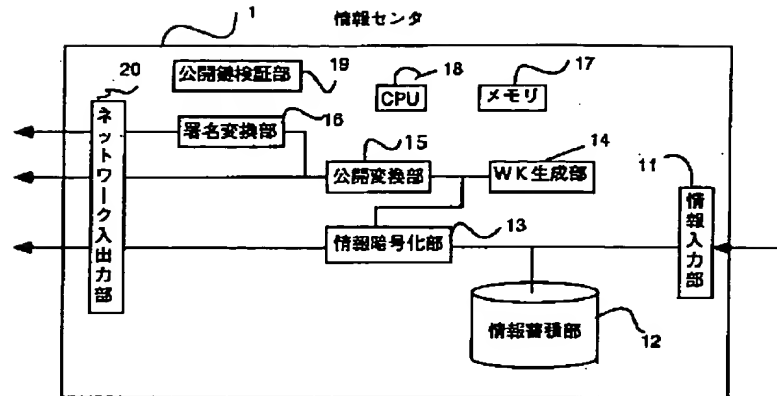
【図1】



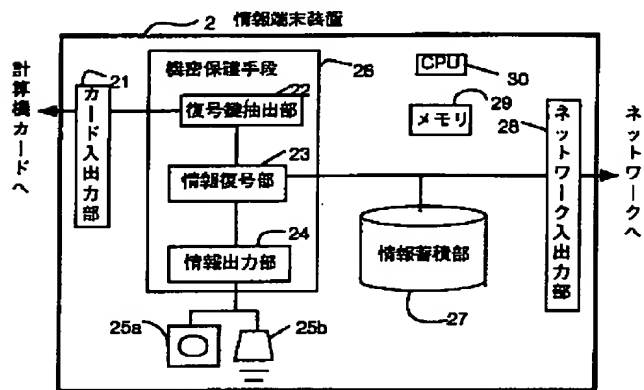
【図6】



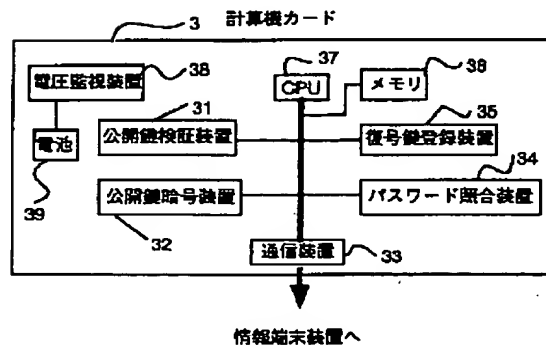
【図 2】



【図 3】



【図 4】

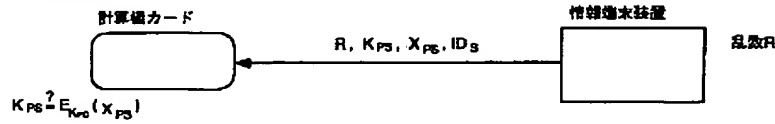


【図 5】

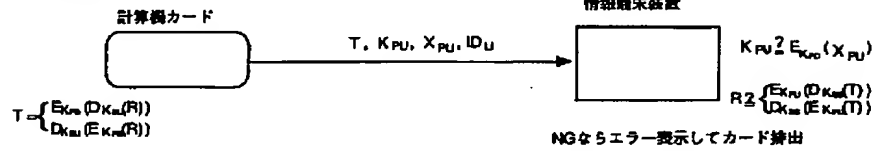
(1) カード挿入 (通信開始)



(2) 相互認証開始



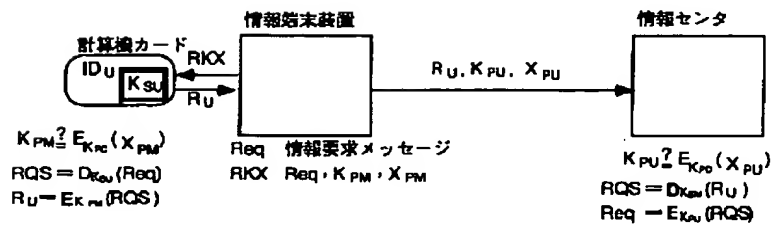
(3) カード応答



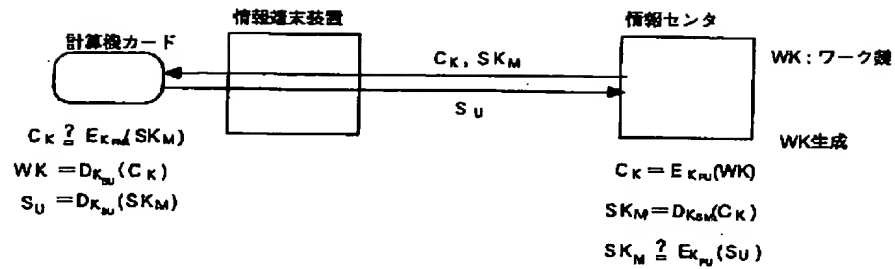
【図 7】



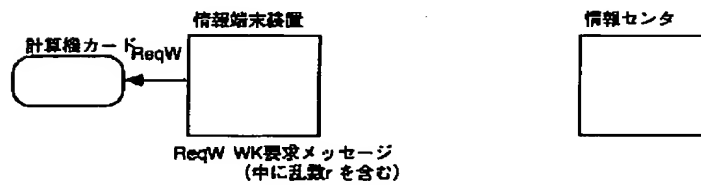
【図 8】



【図 9】



【図 10】



【図 11】

